2-9-2005

Balancing Network Security and Privacy: One Organization's Effort

Priscilla Hutson
Pace University

Balancing Network Security and Privacy:

One Organization's Efforts

Honors Thesis

Priscilla Hutson

Sponsor: Dr. Caroline DeBrovner

Department: Criminal Justice

Spring 2004

Priscilla Hutson

Sponsor: Dr. Caroline DeBrovner

Spring 2004

Balancing Network Security & Privacy: One Organization's Efforts

Honor's Thesis

Introduction

Many organizations are facing the difficult decision of having to choose between respecting their employees' privacy and protecting their computer network. I participated in the process of making this decision at a New York City non-profit organization that requested that I maintain their anonymity, thus I will refer to them as X Organization. X Organization regularly had to deal with viruses corrupting the data in their network and sometimes shutting down the network, inhibiting productivity significantly. The director of the Information Technology Department proposed that changes be made, so a committee was formed to analyze the issue. In this project I researchedthe issue of network security, monitoring internet use, and observed the process in which X Organization developed a solution.

Background on Issue

An organization with internet access runs a high risk of compromising their computer network. Data can be corrupted, confidential information can be stolen, and viruses can paralyze an entire network. Monitoring employee activity

involves questionable legal issues and risk of violating the employees' privacy. An organization must balance the need for monitoring against possible damage to morale, because even an innocent employee may feel spied on.

According to American Management Association's annual survey on workplace monitoring released in April 2001, 78% of large firms in the U.S. are monitoring their employees, but 10% do not notify their employees of this. Monitoring is most common in the for-profit organizations, however 62% of public administrative organizations monitor their employees, and it may have increased since then. Of the 78% of monitoring organizations, 2/3 have disciplined employees for abusing their internet privileges, and more than 1/3 have dismissed employees for these abuses (Skelton).

Options and Alternatives

Internet access being the culprit, the most obvious solution is not to have internet access. However, for many organizations that is not an option. Access can be limited to those who must use it, but if those computers are linked to the organization network, then everyone is just as vulnerable. A quality Information Technology (IT) staff can take many measures to reduce the risk through firewalls, anti-virus software, and an up-to-date operating system, yet the human element of the rest of the organization still poses a threat to the security of the network.

When morale is a top priority, training appears to be the best approach. Education about the policies, why the policies exist, and what they can do to help protect the network as well as their privacy is helpful regardless of the decisions made. Any way to include the staff in the making of changes eases the

transition. Many employees lack the understanding of how computer systems operate and therefore may not foresee risks. The fact that passwords do not equal privacy and that simply viewing a website can bring down the entire organization's network are surprising to many employees. Employee understanding of what seemingly innocent actions can lead to and how the monitoring process works also shows them that the organizations is considering their feelings and value them enough to take the time to respectfully explain everything (Peticolas & Heslin).

Several small things can be done to help protect a network; such as the one's that X Organization will be doing (See Appendix A). These changes enhance the security of a network; however they do not replace the protection from a quality monitoring process.

Why Monitor?

Most companies monitor the internet use of their employees out of fear of liability (Skelton). An employee can sue an employer if they are exposed to offensive material on a coworker's screen. Several hot topics of today's legal departments can quickly become potential law suits due to improper use of the internet by an employee. Sexual harassment is common in the workplace already, but with free pornography rampant online combined with a cubicle or pod environment, the company is extremely vulnerable to sexual harassment claims. If an employee is exposed to offensive material on a coworkers screen, that employee has a case for a hostile working environment. Offensive material can include pictures as well as discriminatory jokes. Many offices also have

shared printers, so if someone is brave enough to print any offensive material and leaves it on the printer long enough for someone else to get to it first, yet another hostile working environment claim may befiled.

Another liability risk is copyright infringement. Employees can illegally download music and movies with programs like Kazaa and that activity is traceable to the organization's network. The music industry has failed at suing individuals for having illegal copies of songs, they win the cases but concentrating on individuals is not cost effective and not scaring others enough to slow the illegal downloading, so the music industry is now targeting service providers. An organization with a network is considered a service provider since it provides internet access to multiple computers, therefore ifemployees download illegal material, the company is held responsible.

Even if a company wins these suits, the cost of legal consultation and litigation is avoidable if the company takes measure to prevent the exposure of offensive material. Policies alone will not stop some employees from venturing into inappropriate material at the office. It is dangerous to rely on employees to monitor themselves, so a company may be safer blocking known offensive websites and monitoring employee internet activity.

X Organization recognized and discussed each of these reasons to monitor the internet use within the organization; however they consider the above reasons a pretext to network security. Adult websites, entertainment sites (jokes, stories, movies), and hacker sites tend to install viruses onto a computer simply by visiting the site. Viruses are also often disguised as music and movies in free downloading programs and websites. X Organization prefers to trust its

employees with not exposing coworkers to offensive material, but when it comes to protecting the network, the whole organization can be paralyzed until it is fixed, so they do agree that something must be done. X Organization is not concerned about trade secrets and propriety information since part of their mission is to share everything they learn, however for-profit companies tend to be very concerned with it.

An immediately perceived problem with internet access is productivity. What if the employees surf and shop online all day and do not get their work done? Productivity can be inhibited by an employee abusing their privileges, but taking away the internet or blocking any non-work related site can also inhibit productivity by angering the employees. Many errands can be taken care of in a few minutes online that would otherwise absorb someone's day, so removing internet access is not necessarily the most efficient solution. What about employees who abuse the privilege? Monitoring is an ideal solution for a productivity concern. Printed out logs will show how much time each employee spent surfing and what sites they were visiting. This could be useful when doing performance reviews (Skelton).

Is it a violation of privacy to monitor an employee's internet activity at the office? It is only illegal if the employee has a reasonable expectation of privacy. "It has been debated and resolved that private employers are permitted to monitor the Internet use of their employees." (Josan). This resolution has not been thoroughly tried and tested and it can still be deemed as an invasion of privacy if the employees are not notified that the monitoring is taking place.

Risks of Monitoring

The first concerns to be addressed are dealing with the human resources perspective. Appearing paternalistic and giving employees the impression that they are not trusted, by babysitting them in cyberspace, can be antiproductive as well as unpleasant (Smith, M. L.). Even an innocent employee may feel uncomfortable knowing he or she is being eavesdropped on, this discomfort is likely to affect his or her mood, communications, and work. Simply reserving the right to search randomly could be considered offensive (Segal, J. A.).

The risks of monitoring employee internet use include the unclear and untried legislation. The right to monitor depends on who and where you are. Government organizations have much stricter regulations. X Organization is a private non-profit that receives government funds and depends on government relationships. This puts X Organization in a grey area that will eventually be clarified with judge-made law (Smith, M. L.). These are risky grounds to tread because violations can carry civil and criminal penalties. Often the deciding factor in the legality of an organization's monitoring is whether or not the organization disclosed the fact that monitoring does take place (Peticolas & Heslin).

Another concern of X Organization's legal department is plausible deniability. If a claim against the organization did arise, X Organization is usually only held responsible if they knew about it, or should have know about it, and did nothing to stop it. If they have the ability to monitor and a claim is brought against them, there is the potential that they should have known about the illegal activity and are therefore held responsible.

X Organization's Decision

As shown in Appendix A, many options are chosen due to IT's recommendation that it is safer to implement several small preventions than to implement one really good one. Appendix A clearly divides and explains the changes, implementation started with the simplest, "No Brainers." The final monitoring decision was to get the server to act as a prophylactic, however not monitor any activity.

Due to the evolving nature of technology, the solution must evolve with it. As new threats are discovered, Organization X must reexamine and change what is necessary in order for this solution to be successful in the long run. The changes should successfully secure the network if it can be implemented before more changes are needed to keep up with the new technologies.

These solutions are appropriate for X Organization if they are communicated clearly and respectfully. X Organization has a staff of liberal, educated people with an environment of working as a team for a great cause, and they expect mutual respect. If X Organization appears not to value these employees or dismiss them as simply staff that should follow the rules, the employees will definitely be offended, and can easily get higher paying jobs elsewhere.

Strengths of X Organization

X Organization has a diverse staff of highly educated people who sincerely believe in the purpose of the organization. Many are fairly young and

still have that fresh energy that drives them to strive toward goals that an experienced professional may dismiss as unrealistic. X Organization thrives on idealism and a passion to change the world. The organization has a history of successfully changing policy and practice in the criminal justice system.

Weaknesses of X Organization

Many of the managers and supervisors are experts in their field and are passionate about their project, but they have little management training. The organization tries to send them to training seminars, but seminars are expensive. Also they have a fairly high turnover rate, not by fault, but by design. Fellows and law students comprise a significant portion of the staff, and the project oriented design of X organization tenders a term of employment of about 2-6 years. Because of this turnover, a high investment in training is not efficient.

X Organization's Culture

X Organization has an immediately noticeable friendly and polite atmosphere. I never got the impression of a hierarchy, even though I know there is one; everyone seems to treat each other as equals. Of course once deeply involved in the everyday interactions and trusted with gossip behind closed doors, you learn that everyone has their natural opinions of people and they tend to gravitate toward their preferred coworkers in times of cooperation. These bonds do not correlate with organizational ranks.

It is also very quiet; it is even policy to go to a conference room to have any sort of meeting, even if it is short and between two people in the same pod.

The pod organization of desks works well to maintain a community atmosphere where everyone is involved and informed of ongoing current projects. The pod walls are about five feet tall, leaving ample space under the high ceilings, which helps keep an open feeling throughout the floor. The pods are much more spacious than a cubicle, and each one allows for ample space for four people without any sensation of being crowded. But also allows visibility to your computer monitor.

Planning

X Organization has taken alert to this issue due to network security fears proposed by the Information Technology Department (IT) as a result of recent data corruption and network paralyzing viruses. A committee was formed of three individuals representing three departments, IT, Legal, and Human Resources (HR), additionally I, the HR intern, attended and participated in each of these meetings. The director of IT represented the technological issues, while the director of HR represented personnel and organizational interests. A fellow from the legal department represented any legal concerns and had to approve each of the new policies. The goal of increasing X Organization's network was then identified and pursued.

The IT director attended the first meeting and gave a list of the changes he wanted to make and he explained what each one was and why it will help. The IT director was never invited to subsequent meetings, even though the Director of HR and the legal department fellow did not understand many factors of the changes. These changes were categorized into three groups (See

Appendix A) in order to sort out what was needed to be done and how much consideration needed to be invested in each change. Once the changes were sorted we decided what was safe with each change, and what problems may occur. The short term goals seemed to be the focus of these changes, with the attitude of "if we do this right it will be done with." Technology changes drastically over the long term, another solution may have to be planned once this one is obsolete, unless X Organization leaves room to successfully evolve the new policies as technology changes.

Organizing

There are several small policies and threats to the system that have been decided and are in the process of being drafted. Once the committee agrees on a change, it is drafted by either the legal representative or the HR Director, and then exchanged between each other and to me. We all read over it and suggested changes. When policies get too tedious, it simply refers the employee to the IT department for individual consideration. Once the legal representative and the HR Director agree on a policy, the legal representative brings it to the legal department meeting for analysis and approval. The legal representative has complained about her department's lack of cooperation with the internet security efforts. This slows the process, but not near as much as the sporadic meetings and spending most of each meeting reviewing what had been covered in previous meetings (Appendix B). The organizing process is yet to be finished for most of the changes. All are at a point of consensus among the committee,

but most are still awaiting the final signature from the president of the organization.

Influencing

X Organization is usually very employee oriented, however it was decided that the security of the network is more important then maintaining the spoiled nature of the staff. Many of the privileges they have grown to expect are unheard of at most organizations, especially in the corporate world, and downloading is against X Organization policy, but has never been enforced. If someone complains, it will be pointed out that it has been against policy for years, and they were nice to let it slide then, but X Organization cannot afford the risk anymore.

A new staff training and orientation has been in a slow process of creation. They plan including all of the new policies and network security reasoning. The orientation has been in planning for years, and it could be another year before it is implemented, so the vital communication factor of changing policy will be missing from the management process in relation to internet monitoring. The fact that the orientation planning has gone on for years begins to show a pattern that the process in which changes are made is inefficient. Due to being tired and burned out, the director of human resources feels the staff “will get over it.” This attitude has the potential to lead to a very poor morale (Certo, 316).

Controlling

X Organization has yet to implement this plan; but most of the objectives have been agreed upon, and the memos and policies have been drafted,

reviewed, and are in the process of being refined. Many of the changes are transparent to the employee, so after any commotion settles, it should slowly become accepted as a norm. What will have to be continually measured is the rate at which the network is compromised and how it was compromised. Currently many try to hack into the network daily and twice a virus has completely shut down the network at X Organization within the last two months. If these rates noticeably decrease as each solution is implemented, then clearly they worked, but it is important that these rates continue to be monitored since technology changes so rapidly, and hackers grow with it. Every time access to your network is blocked, they will find another way in. Policies and practices of X Organization will have to grow and evolve with the technology trends in order for the plan to be successful in the long run.

Conclusion

X Organization has agreed to the balance that works for them, but the existence of the issue still exists. Every organization has to decide on their optimum balance, there is no single right answer. The superficial topic of my research was network monitoring, yet I learned the most from my observance of the decision making process. The organization's intention was to analyze and optimize any change of policy or practice so it leads to maximum benefits with the least consequences. However, the length and tediousness of the process can be so frustrating that the idealistic goal is obscured.

HR was tired of caring about how everyone feels and wants the issue to go away and the IT seems to be the only one who understands that a sense of

urgency is necessary when dealing with issues in technology. After 6 months of planning and organizing, the solution may be insufficient compared to recent advancements. When something goes wrong, IT is blamed, but the process takes so long to get permission to change something that he cannot further prevent network security problems. Now, whenever possible, IT simply changes what he can without permission. He hides anything that management will not likely discover, to avoid X Organization's decision making process.

It is the decision making process itself that lead to this avoidance. It is beneficial for an organization to recognize when it is better to sacrifice the tediousness of the process and just decide. In depth planning may identify many risks and may eliminate some of those risks, however when the planning stage is avoided entirely, all risks go unacknowledged and therefore it is difficult to prevent potential problems. I conclude that the best way to prevent this avoidance is to recognize urgent problems, discuss and decide within one informed meeting, then implement the solution, even if it is a minimalist temporary solution. Further analysis can be done after that if necessary to try to identify problems that may arise and what measure can be taken to prevent them. Employee involvement in these changes, or at least open and honest communication with the staff, will minimize any negative impact on morale.

Bibliography

1. Certo, S. C. Modern Management , 9th Ed. Prentice Hall. (305-318)(481-492).

2. Josan, H. K. & Shah, S. K. (2002). Internet Monitoring of Federal Judges: Striking a Balance Between Independence and Accountability. Hofstra Labor and Employment Law Journal. [FN2].

3. Peticolas, S. and Heslin, K. R. "Electronic Communications in the workplace: A New Challenge in Employment Law." Article. SHRM Legal Report. January 1999. Date of Access: 12 February, 2004. <http://www.shrm.org/hrrescouces/lrpt_published/CMS_000948.asp>.

4. Skelton, V. (2004). "Someone to Watch Over You." Article. HR.com. Date of access: February 12, 2004, <http://www.hr.com/HRcom/index.cfm>

5. Smith, M. L. "Cyber Snooping: Potential new claims leave employers with tough choice." Article. HR.com. Date of Access: 2 February, 2004. <http://www.hr.com/HRcom/index.cfm>.

6. Segal, J. A. "Security vs. Privacy." Article. HR Magazine. 47.2. February 2002. Date of Access: 2 February, 2004. <http://www.shrm.org/hrmagazine/articles/0202/0202legal.asp>.

7. X Organization. Internship from September 2003 May 2004.

Appendix A

(from X Organization meetings)

"No Brainers"	Middle Ground	Difficult Issues
Password Security Employees must change password every 90 days	**Computer Lockup** Limit some Administrative Rights for all employees (system settings, add/remove programs). Remind people about policy against downloading programs.	**Internet Server:** We should get additional server to handle Internet traffic. We should not block employees' access to any sites, but instead provide education to employees about sites that are likely to be compromised (allow self-monitoring). No analysis of employees' Internet usage (monitoring problems, civil liberties concerns).
External Laptops: ***Non-* Employees*** Supervisors must notify IT when non-* people wish to bring their own computers and connect to *'s network. IT must check those computers to make sure that they have adequate security. If not, those machines cannot be connected to *'s network until they are properly equipped. * staff will not do this for them, unless their grant will pay for it. **** Employees*** * employees should not bring home laptops to connect to *'s network unless extraordinary circumstances so justify. These employees must notify IT and ensure that their computer is adequately protected before they can plug into the network	**Current VPN Users** IT will create protocol regarding firewalls and virus scanning, and will train employees who use VPN to update and maintain security on a regular schedule	**New VPN Access:** Who should get to use it? What controls do we/can we put on VPN users and how should we outline their responsibilities? What about consultants with VPN access? When do we cut them off? (Decision held pending IT development of VPN policy).
	Mailbox Upgrade Give people more space on the e-mail server and institute archive policy, train people to use archives more and mandate regular clean up policy.	**Terminated Employees:** With few exceptions, employees' * email accounts will be closed one month after they leave *, and messages will not be forwarded. Employees are expected to notify colleagues and friends that they will not be reachable at * after a certain date and to provide alternate contact information. *Exceptions:* This policy may be altered on a case-by-case basis for consultants and others who may require an on-going * e-mailbox. Each of these individuals must consult with HR and IT about their plans and special needs, or else the default policy outlined above will kick in. (* has discussed with *)
		Outside Email Should we prevent people from logging in to other systems directly or setting up pop-3 to bypass the Exchange server? Forwarding to the * account or using web-based email applications would still be permitted. (Decision tabled for later discussion).

*Names Removed

Appendix B

Meetings at X Organization

Date: 1-27-2004

Present: Director of Human Resources (HR)

Director of Information Technology (IT)

Legal Department Fellow (Legal)

Human Resources Intern (Priscilla)

Discussion: Determine scope of issues

1. Should we get a new server?
    - New 'prophylactic' server (storm drain)
    - Wouldn't take longer
    - Server is a Gateway- would have to ask for permission to get an exception to blocked sites
    - Problem- he'd have access to all, know who goes where and when
    - Firewall is like a front door, the server protects back door
2. IT explains list of suggestions and why they are necessary

    He says it is better to have several small protections then one wholehearted solution.

*IT leaves

3. Issues divided suggestions into chart (Appendix A)

Date: 2-9-2004

Present: Director of Human Resources (HR)

Legal Department Fellow (Legal)

Human Resources Intern (Priscilla)

Discussion: Chart reviewed and updated (Appendix A)

1. Terminated issue-done
2. New VPN users-
3. Separate server o handle net traffic?
    - Get server for safety? Yes
    - Ability to track use? We don't want analysis or reports
    - Would open mgt monitoring problems
    - Plausible deniability- X Org. not responsible if we don't know what was occurring, but if we SHOULD HAVE KNOWN, then we are liable
    - Can we get server and stop there?
    - Solution- get server, no blocking, no tracking (reports) employee education
4. IT credibility questioned- wanttoknow our realistic risk, not worst case scenario-what we believe IT is giving us
5. No Brainers- done entirely as IT asked
6. MiddleG round- combos add up to a lot more security
    - If Middle Ground takes care of so much, what % is left that difficult issues are supposed to cover?
7. VPN- make a X Org. policy- HR responsibility

Date: 2-17-2004

Present: Director of Human Resources (HR)

Legal Department Fellow (Legal)

Human Resources Intern (Priscilla)

Chief Operating Officer (COO)

Discussion: Issues and progress presented to COO

1. Legal says many issues need to be checked into before implementing
2. Now- X Org. has a firewall on each computer, yet things still get through
3. Dangerous ground (Server)
    - Adding filters, ability to track, reports of activity =mo nitoring
    - Monitoring clashes with X Org. culture
    - Civil liberty issues-1st Amendment assumption of privacy
    - X Org. stands for freedom and human rights
    - Gatekeeper function
    - more X Org. cultural concern then legal issue
4. Summarize prior meetings-cover all issue & potential solutions
    - Still want realistic assessment of risk
5. Password- annoying, but automated 5 day warning to change it
6. External laptops-issue origin Chinese visitors plugged in here
    - 2 separate policies
    - Diagnostic tools (Norton etc) must be there, if not, X Org. will put the programs on only if project can afford to pay for time & license

- Ideas- re-use license- uninstall and re install
- License fee? Short term? Set up at a X workstation

7. Middle Ground- Computer Lockup
    - Current policy does not allow downloading, everyone does anyway
    - Kazaa liability, viruses
    - Administrative rights
    - Warning- go around- remove
8. Middle Ground- VPN- discussed and agreed during summary
9. Difficult Issue- President signed off on Terminated Employee policy
10. Difficult Issue- Pop3
11. Difficult Issue- Server-no blocking- employee education on issue
12. Priscilla asked to find out other non profits' solutions (Survey)

Date: 3-23-2004

Present: Director of Human Resources (HR)
Legal Department Fellow (Legal)
Human Resources Intern (Priscilla)

Discussion: Chart covered again and progression discussed

1. Priscilla's survey results presented (Appendix C)
2. Privacy added to policy 5.5 (X Org. internet policy)
3. Can-Spam act

- Put line in policy, probably not X issue
- ban sending spam in 5.5

4. Employer access to Email
5. Software audit
    - Policy 5.5 in X manual—change 1st sentence
    - Trade Association- anyone can file a complaint, and we are audited
    - Exclusion in law for not work related
6. Computer lockup policy
7. Password security
    - Writing
    - Steps to take
    - When to implement
    - Notification
8. VPN- isn't really used, only remote access is used
9. Terminated employees-who's has been a problem

Date: 3-25-2004

Present: Director of Human Resources (HR)

Legal Department Fellow (Legal)

Human Resources Intern (Priscilla)

Discussion: Updates on progress

1. Password will happen 1st, but after building shut down
    - Legal-policy draft

- Will be a level of disruption among staff, will eventually be accepted as “just the way it is”
- (as of 5-13-2004 password solution not implemented)

2. Software - take it all away?
   - IT now says keep AIM & Palms, mostly worried about music & unlicensed software
   - Not lock up until audit
   - Policy- HR wants to keep it simple and not mention exceptions. No “this is ok, this is not.” They can ask IT for what is not ok.

3. Legal Fellow- not getting support (feedback) from Legal Dept on drafts on policies

4. Terminated employees solution- mention in handbook and discussed in exit interview.

5. Went through sample policies and my research on internet monitoring
   - A Organization- maintains standard audit software to monitor system use
   - B Organization- policy back pedals, strangely worded
   - C Organization- “Employees with computer access automatically waive any right to privacy in their electronic communications.”
   - HR likes standard SHRM.org internet use policy
   - HR does not want to require signed acknowledgments

- HR does not want to communicate “why’s” to employees- has potential for lowered employee morale and mistrust.

Date: 3-25-2004

Email From: Legal Department Fellow (Legal)

Email To: Director of Human Resources (HR)

Human Resources Intern (Priscilla)

Subject: Draft of memo explaining new passwords

1. Through email discussed and concluded not to put the password solution into written policy, in time it will just become common practice

Date: 4-8-2004

Email From: Legal Department Fellow (Legal)

Email To: Director of Human Resources (HR)

Human Resources Intern (Priscilla)

Subject: Likely the final draft of policy 5.5 (X Organization internet use policy)

Appendix C

Internet Monitoring Survey Results

Summary	
Participants	23
Don't Monitor	70%
Do Monitor	22%
Right Reserved	43%
Policy Restriction	74%
Block Sites	26%

Detailed Results

Organization	Do you monitor?	Notification of Monitoring
A		right reserved
B	n	na
C		
D	n	policy permits monitoring, sign receipt
E	n	
F	n	n
G	YES	mentioned at orientation, asked if agree
H	n	
I	YES	in handbook, which is signed as whole
J	n	
K	n, right reserved	in handbook, which is signed as whole
L	n	n
M	n	na
N	Y; rarely, if problem	right reserved in handbook, no signing
O	n	n
P	n	n
Q	n; informally, not logs	right reserved in handbook, no signing
R	n	n
S	YES	sign policy at orientation
T	n	na
U	n; not individually	right reserved in handbook, no signing
V	n	
W	YES	y; only a few even have access

Detailed Results Continued

Organization	Do you restrict internet use via policy?	Block Websites?
A	y*	
B	y; limited personal use*	n
C	y *	
D	y	n
E	y; self reported	y; certain porn sites
F	n	n
G		y; IT screening
H	y; must agree to log on to use of business only	yes
I	y; attempts to access inappropriate sites	y; anything not for kids
J	y; to use responsibly	n; nature of business, can't
K	y*	y; Sonic Firewall, block a ton
L	n	n
M	y	n
N	y; business only, as for list serves	y; firewall, eBay maybe more
O	n	n
P	y	n
Q	y; no download, personal gain, chat, or offensive materials	n
R	n	n
S	yes	unsure
T	y; certain activities such as porn not allowed	n; block incoming spam
U	y; not written, memos remind about no downloading music etc	n; virus software on server
V	n	
W	n; but updating	n; may get flagged

*we have a copy of the policy